UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,049	03/04/2002	Robert C. Chang	SANDP015	7791

10027 7590 05/31/2007
ANDERSON, LEVINE & LINTEL L.L.P.
14785 PRESTON ROAD
SUITE 650
DALLAS, TX 75254

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/092,049
Filing Date: March 04, 2002
Appellant(s): CHANG ET AL.

Rodney M. Anderson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on January 17,2007 appealing from the Office action mailed on May 11, 2006 and August 30,2006 finally rejecting claims 1-3, 5-8,11-13 and 17-24.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

- **Claims 1,3, 5-8,11-13 and 17-24** stands rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al. (hereinafter referred as Jones) (U.S. Patent No 5,623,637) in view of Tatebayashi et al (hereinafter referred as Tatebayashi) (U.S. Patent No 6,859,535) (filed on October 15,1999).

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,623,637	**Jones**	04-1997
6,859,535	**Tatebayashi**	02-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. **Claims 1,3, 5-8,11-13, 17-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al. (hereinafter referred as **Jones**) (U.S. Patent No 5,623,637) in view of Tatebayashi et al (hereinafter referred as **Tatebayashi**) (U.S. Patent No 6,859,535) (filed on October 15,1999)

2. **As per claims 1, 8, 13 and 20-21 Jones discloses a method for accessing encrypted information stored in a flash memory storage device [Column 6, lines 11-12]**(encrypt the data prior to storing the data in the common memory array 150 and accessing the data by decrypting the data back into its original form from the storage device 150) **by operating a host system** [figure 2, ref. Num "110"] **in communication with a reader** [figure 2, ref. Num "250"] **the reader including a memory storing a key according to which the information stored in the flash memory storage device is encrypted.** [Abstract; column 6, lines 5-16 and column 3, lines 51-52] (As explained on the abstract and column 6, lines 5-16., the key value is

stored on the smartcard/adapter and obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150" and this memory is indicated to be a flash memory at column 3, lines 51-52]

Inserting the flash memory storage device [figure 1, ref. Num "150" and figure 2, ref. Num "150"] **into the reader** [figure 1, ref. Num "250"] (flash memory are inherently inserted and removed/detached from the floppy disk driver/reader of the host computer. For instance, floppy disk which stores data, are inherently inserted and removed/detached from the floppy disk driver/reader located in the host computer)

Forwarding an access code from the host system to the reader. [Column 5, lines 59-61; figure 2, ref. Num "309" and figure 3] (The driver software prompts the user with a request for a valid password which, when entered is sent via the data buffer)

Responsive to the access code being valid for the reader , obtaining the key from the reader [column 6, lines 9-10; column 5, lines 64- column 6, lines 21 and figure 2 and 3] (if the password/access code is found to be valid after comparing with the password stored in the reader/EEPROM 257 then the key value is stored on the smartcard/adapter is obtained/fetched form the EFPROM "257")

Decrypting the information stored on the flash memory storage device using the key and forwarding the decrypted information to the host

system.[Column 6, lines 9-14 and column 5, lines 64-column 6, lines 14; figure 2 and 3] (As explained on the abstract and column 6, lines 5-16., the key value is stored on the smartcard/adapter/reader is obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150"]

- **Jones** does not explicitly disclose inserting the flash memory storage device into the reader.

However, in the field of endeavor **Tatebayashi** discloses

Inserting the flash memory storage device into the reader. [Column 18, lines 9-29; figure 8, figure 2, figure 6 and figure 18] Furthermore As shown on figure 6 the reader stores a key and as indicated on the abstract, the reader using the key decrypts an encrypted content stored in the flash memory 200]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of inserting the flash memory storage device into the reader as per teachings of **Tatebayashi** in to the method as taught by **Jones,** in order to authenticate the flash memory with the reader.[See **Tatebayashi, column 18, lines 10-12**]

3. **As per claims 3, the combination of Jones and Tatebayashi** discloses the method as applied to claims above. Furthermore Tatebayashi discloses the method further comprising encrypting information using the key, storing the encypted information in the flash memory storage device and removing the flash memory storage device from the reader. [Column 18, lines 9-29; figure 8, figure 2, figure 6 and figure 18 and abstract]

4. **As per claims 5, the combination of Jones and Tatebayashi** discloses the method as applied to claims above. Furthermore Jones discloses the method wherein the access code comprises a first password; and wherein the obtaining step comprises: decoding contents stored in the reader to obtain the key from the decoder content using the first password, responsive to determining that the first password is valid to obtain the key from the decoded content. [column 5, lines 59-column 6, line 14]

5. **As per claims 6-7, 17-19 the combination of Jones and Tatebayashi** discloses the method as applied to claims above. Furthermore Jones discloses the method further comprising: comparing the first password to a second password to determine whether the first password matches the second password wherein the second password is stored in the reader. [Column 8, lines 4-34; Figure 2, ref. Num "320" and column 5, line 61-64]

6. **As per claims 11 and 22-23, the combination of Jones and Tatebayashi** discloses the method as applied to claims above. Furthermore Jones discloses the method wherein the flash memory storage device is one selected from the group consisting of a secure digital card, a Compact Flash card, a multimedia card, smart card and a Memory Stick card. [Figure 1, ref. Num "150" and column 3, lines 51-52]

7. **As per claims 12 and 24, the combination of Jones and Tatebayashi** discloses the method as applied to claims above. Furthermore Jones discloses the method wherein the reader is one of a Universal Serial Bus (USB) reader and a personal computer memory card International Association (PCMCIA) adapter. [Figure 2, ref. Num"250"]

(10) Response to Argument

Appellant's argument filed with the Appeal brief, on January 17, 2007 have been fully considered but they are not persuasive.

Referring to the independent claims 1, Rejections - 35 USC § 103,

Appellant on page 8, second paragraph up to page 9, second paragraph argued that the secondary reference used by the examiner, namely Tatebayash does not indicate the fact that the reader is connected to the host computer when it is accessing the contents of the memory card. Appellant in particular pointed out figure 3 of the secondary reference, Tatebayash, to support his argument.

Examiner first considered the Appeal brief written on page 8, second paragraph up to page 9, second paragraph **in support of the above argument.**

For instance, Appellant on page 9, second paragraph has presented the following argument.

"...Furthermore, ***there is no teaching in the Tatebayashi et al. reference regarding the connecting of this reader to a host personal computer to read the memory card****....Appellants therefore submit that the final rejection of claim 1 and its dependent claims, as unpatentable over the combination of the Jones et al. and Tatebayashi et al. reference, could only have been made through the improper hindsight use of Appellants' own teachings."*

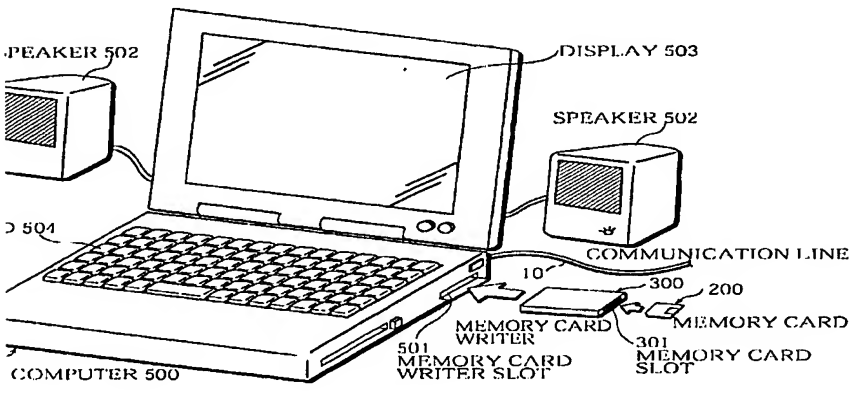
Examiner disagrees with this argument.

First of all, Examiner would point out that the secondary reference on the record namely Tatebayashi et al on column 51, lines 36-column 52, lines 11 and figure 2, discloses the following.

"In the above examples, **after a recording medium device, such as a memory card, is connected to an access device, such as a memory card writer and a memory card reader, each of the recording medium device and the access device judges whether the other device is an authenticated device. Only if both of these devices judges that they are connected to authenticated devices, digital contents are transferred between the recording medium device and the access device. However, the following operation may be performed**. When contents are sent from the access device to the recording medium device, the access device judges whether the recording medium device is an authentication device and, only if the judgment result is affirmative, sends the contents to the recording medium device. In this case, the recording medium device does not judge whether the access device is an authorized device. On the other hand, when contents are sent from the recording medium device to the access device, the recording medium device judges whether the access device is an authorized device and, only if the judgment result is affirmative, the recording medium device sends the contents to the access device. In this case, the access device does not judge whether the recording medium device is an authorized device. This modification is based on the concept that the authentication of a target device by a source device prevents contents that are properly downloaded from being used without proper authorization. In the above examples, **the access device is a memory card writer or a memory card reader. However, the access device may doubles as the memory card writer and the memory card reader.** More specifically, **the access device that doubles as the memory card writer and the memory**

card reader is connected to the personal computer shown in FIG. 2 and a memory card is inserted into the access device. With the personal computer 500, a user obtains contents, such as music data, from the outside via the communication line 10 and writes the contents in the memory card through the mediation of the access device. Also, with the personal computer 500, the user obtains contents from the memory card through the mediation of the access device and reproduces the obtained contents"

For clarification, Examiner also submits diagram (figure 2) disclosed on the secondary reference namely **Tatebayashi et.**



U.S. Patent Feb. 22, 2005 Sheet 2 of 35 US 6,859,535 B1

From what is disclosed/shown above, It is undoubtedly clear that the access device shown on figure 2, ref. Num "300" can either be a writer or reader or both as explained above on column 51, lines 64-lines 67. Furthermore this access device/reader/writer is also connected to a host personal computer shown on figure 2, ref. Num "500" **and the memory card is inserted into the access device/reader** to read the flash memory storage device so that the user of the personal computer 500 obtains contents form the memory card through the mediation of the access device/reader and reproduces the obtained contents. [See column 51, lines 64-column 52, lines 11]

Unlike the Appellant's argument, in fact contrary to the Appellant's argument, the secondary reference on the record, namely Tatebayashi et al, not only discloses that the memory card shown on figure 2, 200 is inserted into the access device/reader/writer shown on figure 2, 300 but also this access device/reader/writer shown on figure 2, 300 is connected to the personal computer shown on figure 2, 500.

Once the Examiner indicates the above fact, the examiner would proceed and respond to appellant's argument starting from the beginning.

Referring to the independent claim 1, Rejections - 35 USC § 103,

Appellant argued that the Examiner has failed to establish a prima facie case of obviousness relative to claim 1, because there is no suggestion from the prior art to combine the teachings of the Tatebayashi et al. reference with those of the Jones et al. reference, in such a manner as to reach independent claim 1. Appellants therefore submit that the final rejection of claim 1 and its dependent

claims is in error and should be reversed.(See appellant's brief on page 5, 3rd paragraph)

Furthermore Appellant argued that the motivation alleged by the examiner is in error because that the specific motivation is not present in the alleged combination of references.

Examiner **considered the Appeal brief written** on page 7, paragraph 2nd up to page 9, first paragraph **in support of the above argument.**

Examiner disagrees with this argument.

Examiner would point out that the primary reference namely Jones et al on column 6, lines 22-31 and figure 1, discloses the following.

"All of the operative circuitry making up the memory card 100, with the exception of the attribute memory 190, the common memory array 150, and the smartcard I.C. 250, is preferably implemented by means of a single, monolithic application specific integrated circuit (ASIC) as indicated within the dashed line rectangle 290 in FIG. 1. By integrating this circuitry in a monolithic integrated circuit, security against invasive attempts to ascertain built-in unlock codes (to be discussed) or to bypass or disable security functions, is substantially improved."

As it is described above,

- The "common memory array 150" shown on figure 1, ref. Num. 150 which is indicated to be a flash memory at column 1, lines 51-52 and
- The "Smart Card IC" shown on figure 1, ref. Num 250 and

- The attribute memory shown on figure 1, ref. Num "190" are not part of the monolithic application specific integrated circuit (ASIC) as indicated by the dashed line rectangle 290 shown on figure 1. Therefore the above description implies the fact that these entities namely the common memory array 150, the smart card IC 250 are physically separate and independent circuits from the monolithic application specific integrated circuit (ASIC) as indicated by the dashed line rectangle 290 shown on figure 1.

Furthermore, the Examiner first shows that the interpretation given to the smart card, as the reader, is correct because the smart card just like the limitation recited in the independent claim 1 **includes a memory storing a key according to which the information stored in the flash memory storage device is encrypted. See for instance what is disclosed on the primary reference on** the abstract and column 6, lines 5-16, the key value is stored on the smartcard/adapter/reader obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150" and this memory is indicated to be a flash memory at column 3, lines 51-52]

- The first question the examiner would raise and subsequently answer is the following.

Is there any prior art, other than the primary reference namely jones et al, which implement these two independent entities namely the "common array memory array 150" and "smart card 250" without enclosing them

in the card shown on figure 1, ref. Num 100, so that the common array memory 150 is inserted to the reader/smart card 250 ?

The answer is Yes, in particular, the secondary reference, namely Tatebayashi et al on column 51, lines 64-67 and column 52, lines 1-11 and figure 2, discloses the following.

"In the above examples, **the access device, shown on figure 2, ref. Num 300 is a memory card writer or a memory card reader. However, the access device may doubles as the memory card writer and the memory card reader." [column 51, lines 64-67** and column 52, lines 1-11 and]

Furthermore the secondary reference discloses the following

"More specifically, **the access device that doubles as the memory card writer and the memory card reader shown on figure 2, ref. Num 300 is connected to the personal computer shown in FIG. 2 ref. Num 150 and a memory card shown on figure 2, ref. Num 200 is inserted into the access device/reader shown on figure 2, ref. Num 300.** With the personal computer 500, a user obtains contents, such as music data, from the outside via the communication line 10 and writes the contents in the memory card through the mediation of the access device/reader/writer shown on figure 2, ref. 300. Also, with the personal computer 500, the user obtains contents from the memory card through the mediation of the access device/reader and reproduces the obtained contents" [column 52, lines 1-11]

- The second question the examiner would raise and subsequently answer is the following.

Is there any advantage/motivation of implementing these two independent entities namely the reader/smart card and flash memory/common array memory of Jones et al without enclosing them in the card 100 so that this memory array/flash memory is inserted into the smart card 250 ?

The answer again is Yes, in particular, the secondary reference, namely atebayashi et al on *column 51, lines 36-63 and* figure 2, discloses the following.

> "After a recording medium device, such as a memory card, is connected to an access device, such as a memory card writer and a **memory card reader**, each of the recording medium device and the access device judges whether the other device is an **authenticated device**. Only if both of these devices judges that they are connected to authenticated devices, **digital contents are transferred** between the recording medium device and the access device. However, the following operation may be performed. When contents are sent from the access device to the recording medium device, the access device judges whether the recording medium device is **an authentication device** and, only if the judgment result **is affirmative**, sends the contents to the recording medium device. In this case, the recording medium device does not judge whether the access device is an authorized device. On the other hand, when contents are sent from the recording medium device to the access device, the recording medium device judges whether the access device is

an authorized device and, only if the judgment result is affirmative, the recording medium device **sends the contents** to the access device. In this case, the access device does not judge whether the recording medium device is an authorized device. **This modification is based on the concept that the authentication of a target device by a source device prevents contents that are properly downloaded from being used without proper authorization."**

Therefore the examiner contend that one of ordinary skill in the art would **undoubtedly motivated to combine** the above feature namely, "the inserting of the memory array into the reader" as per teachings of the secondary reference *Tatebayashi et al* into what is taught by the primary reference namely *Jones et al since such combination would allow the common memory array of Jones et al to be inserted into the reader/smartcard of Jones instead of putting them together in the card shown on figure 1, ref. Num 100, so that the two entities the common array shown on figure 1, 150 and the smartcard shown on figure 1, 250, authenticate each other. And the authentication of the two entities provides the technical benefit of preventing contents that are properly downloaded from being used without proper authorization. [This motivation is explicitly described on the secondary reference shown on column 51, lines 36-63]*

In order to show how each and every limitations of the independent claim 1 and 13, are disclosed by the combination of the two references namely Jones et al and *Tatebayashi et al*, Examiner would also submit the following.

As per claims 1, 8, 13 and 20-21 Jones discloses a method for accessing encrypted information stored in a flash memory storage device

[Column 6, lines 11-12](encrypt the data prior to storing the data in the common memory array 150 and accessing the data by decrypting the data back into its original form from the storage device 150) **by operating a host system** [figure 2, ref. Num "110"] **in communication with a reader** [figure 2, ref. Num "250"] **the reader including a memory storing a key according to which the information stored in the flash memory storage device is encrypted.** [Abstract; column 6, lines 5-16 and column 3, lines 51-52] (As explained on the abstract and column 6, lines 5-16., the key value is stored on the smartcard/adapter and obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150" and this memory is indicated to be a flash memory at column 3, lines 51-52]

Forwarding an access code from the host system to the reader. [Column 5, lines 59-61; figure 2, ref. Num "309" and figure 3] (The driver software prompts the user with a request for a valid password which, when entered is sent via the data buffer)

Responsive to the access code being valid for the reader , obtaining the key from the reader [column 6, lines 9-10; column 5, lines 64- column 6, lines 21 and figure 2 and 3] (if the password/access code is found to be valid after comparing with the password stored in the reader/EEPROM 257 then the key value is stored on the smartcard/adapter is obtained/fetched form the EFPROM "257")

Decrypting the information stored on the flash memory storage device using the key and forwarding the decrypted information to the host system.[Column 6, lines 9-14 and column 5, lines 64-column 6, lines 14; figure 2 and 3] (As explained on the abstract and column 6, lines 5-16., the key value is stored on the smartcard/adapter/reader is obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150"]

- **Jones** does not explicitly disclose inserting the flash memory storage device into the reader.

However, in the field of endeavor **Tatebayashi** discloses

Inserting the flash memory storage device into the reader. [Column 18, lines 9-29; figure 8, figure 2, figure 6 and figure 18] Furthermore As shown on figure 6 the reader stores a key and as indicated on the abstract, the reader using the key decrypts an encrypted content stored in the flash memory 200]

Furthermore **Tatebayashi** discloses the following which meets the limitation of inserting the flash memory storage device into the reader.

"More specifically, **the access device that doubles as the memory card writer and the memory card reader shown on figure 2, ref. Num 300 is connected to the personal computer shown in FIG. 2 ref. Num 150 and a memory card shown on figure 2, ref. Num 200 is inserted into the access device/reader shown on figure 2, ref. Num 300.** With the personal computer 500, a user obtains contents, such as music data, from the outside via the communication line 10 and writes the contents in the memory card through the

mediation of the access device. Also, with the personal computer 500, the user obtains contents from the memory card through the mediation of the access device/reader and reproduces the obtained contents" [column 52, lines 1-11]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of inserting the flash memory storage device into the reader as per teachings of **Tatebayashi** into the method as taught by **Jones,** in order to authenticate the flash memory with the reader.[See **Tatebayashi, column 18, lines 10-12**]. *Since such combination of the two arts would allow the common memory array of Jones et al to be inserted into the reader/smartcard of Jones instead of putting them together in the card shown on figure 1, ref. Num 100, so that the two entities the common array shown on figure 1, 150 and the smartcard shown on figure 1, 250, authenticate each other. And the authentication of the two entities provides the technical benefit of preventing contents that are properly downloaded from being used without proper authorization. [This motivation is clearly described on the secondary reference shown on column 51, lines 36-63]*

In response to Appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the

applicant's disclosure, such a reconstruction is proper. See In re McLaughlin, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

On Appeal brief, page 9, last sentence up to page **11-second paragraph,** Appellant's further argued that the two level of security provided by the inventions is a substantial improvement over a single levels of security provided by the Jones et al and **Tatebayashi** et al.

For instance, the following has been written in support of Appellant's argument.

"Accordingly, to access the contents of the flash memory storage device according to the invention, one must have both a valid access code that is forwarded to the reader, and also must have the reader that contains the encryption key according to which the contents on the flash memory storage device are encrypted. This combination provides important security advantages over conventional secure flash memory systems, because a thief or other unauthorized user possessing the flash memory storage device cannot access its contents without possession of both the reader with the key, and also the valid access code required to retrieve that key.

The two levels of security provided by this invention are a substantial improvement over the single levels of security provided by the Jones et al. and Tatebayashi et al. references. The Jones et al. reference provides only a password security mechanism." [See the appeal brief on page 9, last sentence up to page 10, second paragraph]

Examiner disagrees with this argument.

Examiner would point out that the primary reference/ Jones reference on the record not only provides a valid access code/password that is forwarded to the reader/smart card or single levels of security as argued by the Appellant but also provides/requires that the reader contains the encryption key according to which the contents on the flash memory storage device are encrypted which is second levels of security.

On column 5, lines 59-61; figure 2, ref. Num "309" and figure 3, the following has been disclosed by Jones. "The driver software prompts the user with a request for a valid password which, when entered is sent via the data buffer" and this meets the limitation recited as "providing a valid access code/password that is forwarded to the reader/smart card". Furthermore, on Abstract; column 6, lines 5-16 and column 3, lines 51-52, Jones discloses the following, the key value is stored on the smartcard/adapter and obtained/fetched form the EFPROM "257" and the key is used to encrypt/decrypt information that is to be stored in the memory shown on figure 2, ref. Num "150" and this memory is indicated to be a flash memory at column 3, lines 51-52 and this meets the limitation recited as, "the reader must contain the encryption key according to which the contents on the flash memory storage device are encrypted which is second levels of security".

Furthermore, **Examiner observed** that most of the argument presented by Appellant is targeting the references individually. In response to Appellant's arguments against the references individually (either the primary reference Jones or the secondary reference **Tatebayashi)**, Examiner contends that one

cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Like wise, In response to the Appellant's argument that there is no motivation to combine the reference, Examiner would like to point out that, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Referring to the independent claim 13, Examiner would point out that all the argument presented above is also applicable to the Appellant's argument presented for independent claim 13.

The rest of Appellant's argument is regarding the dependent claims, that are depending on to the respective independent claims 1 and 13.

Appellant argued that *since the independent claims are allowable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claim.*

In response to the above argument by the Appellant, **the examiner replies** that the respective dependent claims stands or falls with the corresponding independent claims 1 and 13.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Samson Lemma
S.L.
05/21/2007

Conferees:

Kim Vu KV

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

ARANI TAGHI T

TAGHI ARANI
PRIMARY EXAMINER